



23. august 2024

D-mærket

# Virksomhedsattest

D-mærkets kontrol af PERSPEKTIVA IT ApS



## 1. Formål og tiltænkte brugere

Denne attest er udarbejdet til PERSPEKTIVA IT ApS ("**Virksomheden**"), dens ledelse og relevante interessenter af Mærkningsordningen for it-sikkerhed og ansvarlig dataanvendelse ("**Mærkningsordningen**"). Attesten er et overordnet indblik i de kontrolmål, der er blevet udtaget til tilsyn, om fremgangsmåden for tilsynet i forbindelse med anmodning eller genanmodning om D-mærket, samt resultatet af tilsynet. Det er Virksomhedens egen vurdering, om de ønsker at dele attesten.

## 2. Uafhængighed

Mærkningsordningens Auditors er uafhængige af øvrig kontrol, og deres beslutninger er uden ekstern påvirkning. Tilsyn og kontrol bliver udført ud fra grundlæggende principper om integritet, objektivitet, faglige kompetencer, fortrolighed samt professionel adfærd.

Virksomheden bliver bedømt og kvalitetskontrolleret af minimum to Auditors.

## 3. Virksomhedens ansvar

Som afslutning på Virksomhedens selvevaluering, og inden tilsynet og fremsendelse af dokumentation gennemføres, har Virksomheden underskrevet en tro- og loveerklæring, hvori de erklærer, at alle spørgsmål og informationer givet af Virksomheden er korrekte.

Derudover finder vilkårene for D-mærket anvendelse, og Virksomheden er forpligtet til at følge dem.



## 4. Information om Virksomheden

### Oversigt 1

<b>Navn på virksomhed</b>	PERSPEKTIVA IT ApS			
<b>Virksomhedsadresse</b>	Højvang 5			
<b>Postnummer</b>	4300	<b>By</b>	Holbæk	
<b>Telefonnummer</b>	88530200	<b>CVR</b>	29616892	
<b>URL</b>	<a href="https://www.perspektiva-it.dk/">https://www.perspektiva-it.dk/</a>			
<b>Branche</b>	Anden it-servicevirksomhed			
<b>Branchekode</b>	620900			
<b>Antal ansatte</b>	<input type="checkbox"/> 0-9	<input checked="" type="checkbox"/> 10-49	<input type="checkbox"/> 50-249	<input type="checkbox"/> 250-999 <input type="checkbox"/> >1000
<b>Nettoomsætning ved seneste regnskab</b>	<input type="checkbox"/> 0-7,9 mDKK	<input checked="" type="checkbox"/> 8-155,9 mDKK	<input type="checkbox"/> 156-313 mDKK	<input type="checkbox"/> ≥313 mDKK
<b>Kontaktperson</b>	Claus Daugaard Hansen			
<b>Titel</b>	Systemarkitekt	<b>E-mail</b>	<a href="mailto:cdh@perspektiva-it.dk">cdh@perspektiva-it.dk</a>	

## 5. Omfang for audit

Mærkningsordningens Auditors kontrollerer Virksomhedens efterlevelse af D-mærkets krav ud fra udvalgte kontrolmål (niveau 3 kriterier) og tilhørende kontrolaktiviteter (krav). De specifikke udvalgte og fortrolige kontrolaktiviteter (krav) fremsendes ved tilsyn og fremgår ikke i denne rapport.

Kontrollen er udført som "point in time" kontrol, hvorfor Virksomheden dokumenterer et øjebliksbillede af Virksomhedens faktiske forhold.

Ved genanmodning om D-mærket vil Virksomheden ligeledes skulle dokumentere "over time", således at perioden fra første tildeling til genanmodning om D-mærket afdækkes.



## Oversigt 2

<b>Kompenserende kontroller</b>	<input type="checkbox"/> [Indsæt krav hvor kompenserende kontroller er benyttet]
<b>Virksomhedstype</b>	<input type="checkbox"/> Gruppe I <input type="checkbox"/> Gruppe II <input checked="" type="checkbox"/> Gruppe III <input checked="" type="checkbox"/> Gruppe IV
	<input checked="" type="checkbox"/> Virksomheden er leverandør af software eller it-tjenester til andre <input checked="" type="checkbox"/> Virksomheden anvender leverandører (som benytter it) til behandling af personoplysninger og / eller forretningskritiske data <input type="checkbox"/> Virksomheden udvikler software <input type="checkbox"/> Virksomheden anvender eller udvikler algoritmer eller AI
<b>Udvalgt kriterie (niveau 1)</b>	<b>Udvalgte kontrolmål (niveau 3)</b>
<input checked="" type="checkbox"/> 1.0 Styring og forankring i ledelsen	<input checked="" type="checkbox"/> 1.1.1 Udpegning af ansvarlig person for it-sikkerhed og ansvarlig dataanvendelse <input checked="" type="checkbox"/> 1.2.1 Overblik over personoplysninger <input checked="" type="checkbox"/> 1.2.2 Overblik over forretningskritiske data <input checked="" type="checkbox"/> 1.2.3 Overblik over it-systemer, tjenester, netværkskomponenter, enheder, software og aktivitetsbaserede algoritme/AI "use cases" <input checked="" type="checkbox"/> 1.3.1 Risikovurdering og -håndtering <input checked="" type="checkbox"/> 1.4.1 Politik for it-sikkerhed <input checked="" type="checkbox"/> 1.5.1 It-beredskabsplan <input checked="" type="checkbox"/> 1.6.1 Politik for behandling af personoplysninger <input checked="" type="checkbox"/> 1.6.2 Politik for dataetik <input type="checkbox"/> 1.7.1 Krav til udviklingsproces
<input checked="" type="checkbox"/> 2.0 Awareness og sikker adfærd	<input type="checkbox"/> 2.1.1 Træn bestyrelsen og den øverste ledelse i it-sikkerhed, databeskyttelse og dataetik <input checked="" type="checkbox"/> 2.2.1 Træn alle ansattes og brugeres viden om it-sikkerhed kontinuerligt <input checked="" type="checkbox"/> 2.3.1 Træn alle ansattes og brugeres viden om ansvarlig behandling af personoplysninger kontinuerligt <input type="checkbox"/> 2.3.2 Træn alle ansatte og brugeres viden om dataetik kontinuerligt
<input checked="" type="checkbox"/> 3.0 Teknisk it-sikkerhed	<input type="checkbox"/> 3.1.1 Beskyttelse af administrative grænseflader, netværk og enheder <input type="checkbox"/> 3.1.2 Kryptering af ekstern netværksadgang <input type="checkbox"/> 3.2.1 Opsætning og vedligeholdelse af korrekt konfiguration <input checked="" type="checkbox"/> 3.3.1 Beskyttelse af administrative brugerkonti <input checked="" type="checkbox"/> 3.4.1 Implementering af beskyttelsesmekanismer mod malware <input type="checkbox"/> 3.4.2 Beskyttelse mod uønskede e-mails. <input checked="" type="checkbox"/> 3.5.1 Kontinuerlig opdatering af software og styresystemer <input checked="" type="checkbox"/> 3.6.1 Procedure for automatisk og jævnlig backup <input type="checkbox"/> 3.7.1 Overvågning af systemaktivitet gennem logning



<input checked="" type="checkbox"/> 4.0 Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse	<input checked="" type="checkbox"/> 4.1.1 Leverandørlivscyklus og risikovurdering <input checked="" type="checkbox"/> 4.2.1 Krav til it-sikkerhed hos leverandører <input checked="" type="checkbox"/> 4.3.1 Krav til persondatabelandling hos leverandører <input type="checkbox"/> 4.3.2 Krav til dataetisk behandling hos leverandører
<input checked="" type="checkbox"/> 5.0 Transparens & kontrol med data	<input checked="" type="checkbox"/> 5.1.1 Oplysningspligt overfor den registrerede <input type="checkbox"/> 5.1.2 Information om samarbejdspartnere, der deles data med <input type="checkbox"/> 5.2.1 Cookie-information og -brugervenlighed <input checked="" type="checkbox"/> 5.3.1 Brugerkontrol <input type="checkbox"/> 5.4.1 Lettilgængelig klagevejledning vedrørende ansvarlig dataanvendelse og it-sikkerhed
<input type="checkbox"/> 6.0 Privacy & security by design & default	<input type="checkbox"/> 6.1.1 Risikovurdering <input type="checkbox"/> 6.1.2 Tag stilling til persondatabelandlings- og sikkerhedsniveau <input type="checkbox"/> 6.2.1 Minimering og begrænsning <input type="checkbox"/> 6.2.2 Separering og skjul <input type="checkbox"/> 6.2.3 Aggregering <input type="checkbox"/> 6.2.4 Persondatabelandling som standardindstilling (indlejring af persondatabelandling) <input type="checkbox"/> 6.2.5 Fuld funktionalitet og persondatabelandling <input type="checkbox"/> 6.3.1 Minimer angrebsflader <input type="checkbox"/> 6.3.2 Højt niveau af sikkerhed som standardindstilling <input type="checkbox"/> 6.3.3 Mindste sæt af rettigheder/rettighedsstyring <input type="checkbox"/> 6.3.4 Kontrol af kode (egen og tredjepart) <input type="checkbox"/> 6.4.1 Implementering igennem udviklingsproces
<input type="checkbox"/> 7.0 Pålidelige algoritmer & AI	<input type="checkbox"/> 7.1.1 Risikovurdering <input type="checkbox"/> 7.1.2 Interessentinddragelse <input type="checkbox"/> 7.1.3 Informationspligt og gennemsigtighed <input type="checkbox"/> 7.1.4 Udfordringsret <input type="checkbox"/> 7.1.5 Nødstop <input type="checkbox"/> 7.2.1 Valg af inferensmetode og forklarlighed <input type="checkbox"/> 7.2.2 Høj kvalitetsdatagrundlag <input type="checkbox"/> 7.2.3 Kontinuerlig evaluering af data og beregningslogik <input type="checkbox"/> 7.3.1 Implementering igennem udviklingsproces
<input checked="" type="checkbox"/> 8.0 Dataetik	<input checked="" type="checkbox"/> 8.1.1 Dataetiske overvejelser



## 6. Forløb af audit

PERSPEKTIVA IT ApS anmodede om tilsyn den 27.03.2024.

Virksomheden fik adgang til Mærkningsordningens udvalgte kontrolmål via D-mærkets tilsynsværktøj den 13.05.2024 med deadline for upload af dokumentation sat til den 28.05.2024.

Mærkningsordningens tilsyn fremsendte den 03.06.2024 sine opfølgninger på baggrund af den uploadede dokumentation til Virksomheden. Tilbage meldingen bestod af enkelte opfølgende handlinger inden for Kriterie 1: *Styring og forankring i ledelsen*, Kriterie 2: *Awareness og sikker adfærd*, Kriterie 3: *Teknisk it-sikkerhed*, Kriterie 4: *Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse* samt Kriterie 5: *Transparens & kontrol med data*.

Virksomheden fremsendte den efterspurgte dokumentation den 21.06.2024. Mærkningsordningens tilsyn fremsendte den 02.07.2024 hertil enkelte opfølgende handlinger, hvortil Virksomheden indleverede dokumentation den 03.07.2024.

Mærkningsordningen afsluttede tilsynet med Virksomheden den 08.08.2024.



## 7. Konklusion

PERSPEKTIVA IT ApS har på generel tilfredsstillende måde dokumenteret efterlevelse af Mærkningsordningens udvalgte kontrolmål.

Tilsynet bemærker, at virksomheden generelt har udarbejdet anvendelige styringsdokumenter, der detaljeret beskriver Virksomhedens tilgang til- og håndtering af deres it-sikkerhed og ansvarlige anvendelse af data. Dokumenterne ses generelt dateret nyligere end ét år, og Virksomheden kan med fordel fortsætte med årlig revision af samtlige styringsdokumenter, for at sikre sig at alle processer og politikker forbliver relevante.

Tilsynet bemærker, at Virksomheden primært baserer sin interne awareness-træning på gennemgang af interne politikker og dokumenter. Virksomheden bør i perioden frem mod næste tilsyn formalisere indhold og proces for awareness-træning, sikre sig at denne tilfører ny og relevant information, samt registrere hvilke medarbejdere der gennemfører træningen og ej.

Tilsynet bemærker, at Virksomheden har formuleret en dataetisk politik baseret på tilvalg af relevante dataetiske principper. Virksomheden bør dog arbejde videre med de dataetiske refleksionsspørgsmål relateret til kriterie 8.1.1.1, og overveje om ændringer og/eller berigelser bør afspejles i den dataetiske politik.

Tilsynet bemærker, at Virksomheden i hele tilsynsprocessen har været imødekommende og at aftalt dokumentation er blevet leveret rettidigt.

Mærkningsordningens tilsyn konkluderer på baggrund af ovenstående, at D-mærket tildeles Virksomheden. Tildelingen gælder for perioden 23.08.2024 til 01.09.2025. Virksomheden kan genansøge om D-mærket, som beskrevet i D-mærkets vilkår.

<b>Lead Auditor</b>	Emil Zeiler Alfsen	<b>Dato</b>	23.08.2024
<b>Underskrift</b>			
<b>Auditor</b>	Stine Randklev Nissen	<b>Dato</b>	23.08.2024
<b>Underskrift</b>			
<b>D-mærketildeling</b>	<b>D-mærket er blevet tildelt</b>	<b>D-mærket er ikke blevet tildelt</b>	
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>Type af kontrol</b>	<input checked="" type="checkbox"/> Point in time <input type="checkbox"/> Over time		